

# Análisis de las Vulnerabilidades: Evaluación de los Requerimientos de Inteligencia del Comandante

**Coronel (R) Clint J. Ancker, III, Ejército de los EE.UU.**

**H**ASTA LOS ataques terroristas del 11 de septiembre al *World Trade Center* y al Pentágono, veíamos la protección de la fuerza, y especialmente el antiterrorismo, como partes integrales de todas las operaciones. Además, la mayor parte de las pautas a seguir para la seguridad de una instalación están incluidas en las normas del Ejército. Esto de acuerdo a la división de responsabilidades, donde los reglamentos establecen principalmente los aspectos administrativos del Ejército, mientras que los Manuales de Campo se refieren a la forma en que el Ejército realiza las operaciones. El 11 de septiembre puede cambiar parte de esto. Una propuesta consiste en hacer de la protección de la fuerza una tarea separada en la Lista Universal de las Tareas del Ejército y proveer al comandante y a su equipo basado en la doctrina las instrucciones sobre cómo realizar esta nueva tarea táctica. A medida que el Ejército trabaja en el cuadro de pensamiento sobre las operaciones de protección de la fuerza, ha desarrollado algunas ideas sobre cómo puede adaptar los conceptos operacionales existentes a esta tarea. Así mismo, el grupo de expertos está estudiando cómo el Ejército necesita poner al día sus ideas acerca de la vulnerabilidad, basándose en el cambio significativo del patrón de ataques del enemigo manifestado en los ataques del 11 de septiembre. Estamos tras la atención de una metodología de análisis de la vulnerabilidad que permitirá a las fuerzas del Ejército disuadir, hacer fracasar cualquier ataque terrorista y manejar mejor las consecuencias de los ataques terroristas.

Los ataques al *World Trade Center* y al Pentágono demuestran que la protección de la fuerza del Ejército debe cambiar. Anteriormente la protección de la fuerza se enfocaba a disuadir o a hacer fracasar ataques de poca magnitud contra objetivos específicos.

Los ataques del 11 de septiembre combinaron dos métodos de operar con los que estamos familiarizados—el del hombre-bomba suicida y el del secuestro de aviones—en un inesperado ataque que rompió con todos los parámetros conocidos y que estuvo dirigido a causar daños en forma masiva y a convertirse en un acontecimiento que llamara la atención mundial. El grupo que llevó a cabo dichos ataques está bien organizado, tiene una férrea disciplina y cuenta con apoyo económico. Los ataques estuvieron muy bien planeados y sincronizados. Los objetivos fueron seleccionados cuidadosamente. Las acciones de todos los que estuvieron involucrados, inclusive las acciones previstas de los pasajeros y de la tripulación de las aeronaves, estuvieron muy bien planeadas. Los ataques del 11 de septiembre establecieron un nuevo modelo de ataque terrorista. El concepto de la protección de la fuerza que tiene el Ejército debe cambiar para poder enfrentar este nuevo modelo de amenaza.

Un aspecto clave de este cambio es el nuevo enfoque con que el Ejército debe evaluar la vulnerabilidad. Muchos de los principios fundamentales de las operaciones militares están aún vigentes, pero las tácticas, técnicas y procedimientos que se usan para aplicar esos principios a este nuevo tipo de amenaza son diferentes. Los conceptos de los requisitos de información crítica que debe tener el comandante (RICC) están formados por requisitos de información prioritaria (RIP), requisitos de información de las fuerzas aliadas (RIFF) y elementos esenciales de información amistosa (EEIA) conocidos por cualquiera que ha usado el proceso militar de toma de decisiones (PMTD). Al adaptar estos términos al análisis de la vulnerabilidad para la protección de la fuerza contra el terrorismo, estamos basándonos en conceptos familiares al mismo tiempo que trascendemos su significado convencional.

Los comandantes visualizan, describen y dirigen las acciones a través de todo el transcurso de las operaciones y el espectro del conflicto. Vital para la PMTD, y especialmente importantes para la protección de la fuerza (PF) de la instalación son los RICC y EEIA. La aplicación de los principios doctrinales de RICC y EEIA tiene tanta relevancia para PF de la instalación como para las operaciones en el campo de batalla; sin embargo, la aplicación de estos conceptos a la PF de la instalación difiere de manera significativa de su aplicación en combate.

El comandante necesita información precisa y oportuna para visualizar, tomar decisiones y dirigir la acción. Los RICC son vitales en este proceso. Los RICC son elementos de información que los comandantes necesitan y que afectan directamente la toma de decisiones y determinan la ejecución exitosa de las operaciones militares. Los RICC determinan y jerarquizan el plan de recopilación de la información, la distribución consecuente de los recursos de la recopilación y las tareas del análisis. Muchos—si no es que todos los RICC—están directamente enlazados con aspectos de la decisión. De esta manera las respuestas a los RICC habilitan al comandante a anticipar decisiones necesarias de una manera oportuna. En la PF interna las decisiones que el comandante toma deben balancear la amenaza, la efectividad de las operaciones y los recursos disponibles.

Desarrollar los RICC para la protección de la fuerza de la instalación comienza cuando el comandante visualiza la operación y, especialmente, el ámbito de la batalla. El comandante tiene que visualizar los factores dentro del ámbito de la batalla. Partiendo de esta visualización inicial, el comandante describe la operación y establece normas para la planificación. Un componente de estas normas para la planificación son los RICC. Para poder comprender la amenaza, el comandante necesita determinar varias cosas; éstas se pueden convertir en RIP.

Los RIP se concentran en la información sobre el enemigo, el terreno y el estado del tiempo. En la PF de la instalación, los RIP se concentran en la evaluación de la amenaza. Durante tiempos de actividad normal los RIP están formulados a grandes rasgos y se refieren a una serie de amenazas posibles. La recopilación basada en los RIP para la PF depende mucho más de agencias civiles que de recursos orgánicos. Al Ejército le está terminantemente prohibido recopilar información sobre amenazas internas. Las buenas relaciones con agencias civiles locales y nacionales resultan críticas cuando las instalaciones actúan contra las amenazas internas. Por lo tanto, unas relaciones sólidas con estas agencias

resultan críticas. El resultado será la predicción acerca de las operaciones terroristas y un cálculo de los objetivos potenciales de los terroristas. Armados con estos elementos, los comandantes pueden hacer algunos cálculos que se puedan aplicar a la fórmula descrita anteriormente. Así, los RIP realistas para la PF de la instalación tienen como propósito comprender lo que el enemigo está intentando hacer y luego determinar cuan amistosamente pueden responder las fuerzas aliadas. En suma, los RIP guían el análisis de la vulnerabilidad.

La naturaleza episódica de la amenaza terrorista, la falta de un enemigo claramente identificado, la falta de una capacidad orgánica de ostentación de información y una diversidad de fuentes, hacen que la obtención

**Debemos imaginar la manera más probable en que los terroristas usarán sus recursos para lograr sus metas a corto y a largo plazo. Los analistas deben estar imbuidos de la filosofía, el pensamiento y la cultura de los terroristas.**

de los RIP sea un verdadero desafío. Desarrollar la habilidad de llegar y penetrar fuentes de información es una destreza fundamental para el personal encargado de la instalación.

A causa de la imposibilidad de dirigir esta recopilación de RIP, la instalación debe dedicar recursos considerables a analizar la información disponible en un esfuerzo por predecir posibles amenazas basándose en los datos obtenidos por la inteligencia. Esto requiere de analistas extremadamente habilidosos que de la información, que a menudo es incompleta y no es fidedigna, puedan descubrir posibles amenazas. Un desafío adicional, viene a ser la falta de personal bien adiestrado en inteligencia y seguridad en el grupo responsable de la instalación para analizar y afinar la información recopilada. Algunas consideraciones críticas para enfocar los RIP en estos tipos de operaciones son:

**Determinar los objetivos de los terroristas.** Debemos entender los objetivos de los terroristas a corto y a largo plazo. De estos podemos inferir los efectos que esperan lograr e identificar los blancos que les permitirían lograr esos efectos.

**Determinar la capacidad de los terroristas.** Este paso implica determinar los métodos más probables que los terroristas podrían usar para atacar el blanco. Implica un análisis de los métodos usados anteriormente, pero además requiere imaginación para combinar métodos en nuevas formas, o inferir tácticas totalmente originales.

**Determinar las intenciones de los terroristas.** Debemos imaginar la manera más probable en que

los terroristas usarán sus recursos para lograr sus metas a corto y a largo plazo. Los analistas deben estar imbuidos de la filosofía, el pensamiento y la cultura de los terroristas. Al irse definiendo más claramente la amenaza, los RIP cambian para concentrarse ahora en las posibles amenazas y en determinar sus posibles blancos y los medios para atacarlos.

Los RIFF son esos elementos de información sobre las fuerzas aliadas que el comandante de la instalación y su equipo necesitan. En la PF de la instalación, los RIFF tienen dos grandes áreas: determinar la vulnerabilidad y determinar la capacidad de respuesta. Primero, el comandante de la instalación y su equipo necesitan información sobre la vulnerabilidad de la instalación ante los ataques terroristas. Durante las operaciones rutinarias esto se manifiesta como un conocimiento general de los puntos vulnerables. Las vulnerabilidades deben ser determinadas teniendo en cuenta los modelos de operaciones terroristas que se conocen, pero también debe establecerse con el criterio de qué causaría mayores daños en caso de que fuera blanco de un ataque terrorista. Mientras que la primera es relativamente simple y tiene como base el análisis de acciones terroristas del

### **Supón que tu enemigo está pensando como tú, y está realizando una posevaluación de las acciones y está buscando las formas de convertir tus medidas de seguridad en vulnerabilidades.**

pasado, la segunda es mucho más difícil de establecer. Determinar la vulnerabilidad requiere imaginación así como también la capacidad de pensar desde la perspectiva de la planificación de un ataque terrorista asimétrico y no convencional contra la instalación. Este análisis de la vulnerabilidad es un proceso continuo.

De la misma manera que con los RIP, cuando una amenaza concreta es identificada, el comandante cambia sus RIFF para concentrarse en aspectos específicos y objetivos conocidos del supuesto ataque terrorista. El comandante debe entonces dirigir las acciones a eliminar o mitigar los efectos potenciales de la amenaza con respecto a los supuestos puntos vulnerables.

La segunda área de los RIFF para la PF es la capacidad del comandante para responder a un ataque terrorista. Durante las operaciones rutinarias, los RIFF deben en lo general concentrarse en la capacidad del comandante para responder a una extensa gama de amenazas. Cuando las amenazas empiezan a tomar una forma más definida, los RIFF deben concentrarse en la capacidad del comandante para disuadir o responder a la amenaza.

El comandante de la instalación usa las respuestas de

los RIP y RIFF para tomar decisiones. La mayoría de las veces sus decisiones sobre la PF se clasifican en dos categorías: implementación de las medidas de seguridad y la ejecución de una respuesta a un ataque terrorista y a sus consecuencias.

Durante operaciones rutinarias el comandante evalúa su actitud de seguridad basado en las amenazas conocidas o supuestas. Las medidas de seguridad están basadas en el balance de la habilidad del comandante para manejar los asuntos normales y la probabilidad de un ataque. Generalmente el objetivo es minimizar la interrupción de la vida diaria que trae como consecuencia la probabilidad de un ataque. Otras decisiones están dirigidas a perfeccionar la capacitación del comandante para responder a ataques terroristas. Si un análisis de acciones terroristas del pasado y potenciales acciones futuras, requiere de equipos de respuesta específicos, tales como equipos capaces de resolver una situación de rehenes, o de hacer una limpieza después de un ataque biológico, el comandante debe determinar si tiene equipos suficientemente entrenados y equipo disponible. Puesto que las posibles amenazas siempre van a ser superiores a los recursos disponibles, el comandante debe usar las respuestas a los RIP (amenazas potenciales) y los RIFF (puntos vulnerables potenciales) para determinar dónde emplear los escasos recursos. Además de estas decisiones, el comandante debe establecer los EEIA.

Una vez que la instalación haya determinado sus puntos vulnerables, el comandante usará la EEIA para proteger la mayor cantidad de información crítica que sea posible. Los EEIA son información crítica sobre fuerzas aliadas que si fuera descubierta por el enemigo pondría en peligro, llevaría al fracaso o limitaría el éxito de la fuerza aliada. La seguridad de las operaciones (SEGOP) es el proceso que los comandantes siguen para proteger los EEIA. En condiciones normales la SEGOP consiste en acciones necesarias para evitar que una amplia gama de información útil caiga en manos equivocadas. Si bien la mayoría de los soldados y los civiles que trabajan para el Departamento del Ejército están familiarizados con los procedimientos normales de la SEGOP para operaciones de combate, no hemos desarrollando la misma conciencia de la SEGOP para medidas antiterroristas. Los EEIA para la PF interna contra el terrorismo es también una derivación del análisis de la vulnerabilidad. Guiado por el análisis de la vulnerabilidad, el comandante y su equipo tratan de predecir los posibles efectos de filtración de información sobre la seguridad de la instalación y luego crear las medidas necesarias para evitar que esta información se divulgue.

A medida que las respuestas identifiquen con más

claridad la amenaza, el comandante llegará a conclusiones con respecto a la implementación de la SEGOP y de las medidas físicas de seguridad contra la amenaza concreta. Esto incluirá el establecer normas más estrictas para el control de acceso, proteger al personal y los recursos clave, y posiblemente ensayar simulacros de respuesta. Además, basado en la amenaza específica, el comandante revisará los EEIA para proteger la información que ayudaría a los terroristas a realizar el ataque.

Una parte integral del PMTD es el análisis de los riesgos. El análisis de los riesgos da al comandante un medio para balancear los requisitos de la PF con

**Proteger nuestras instalaciones con el uso de la fuerza será una parte importante de nuestras vidas en un futuro inmediato. Si queremos tener éxito en nuestra empresa, tendremos que ser tan creativos como nuestro adversario.**

el cumplimiento de la misión. Cerrar la instalación y crear una “fortaleza” proporcionaría una seguridad casi hermética. Por cada serie de medidas de seguridad adoptados deja siempre se mantiene un riesgo residual. Si este riesgo resulta excesivo, el comandante debe implementar medidas adicionales para reducirlo. Un riesgo de este tipo siempre debe balancearse con la necesidad de seguir adelante con las operaciones.

Las prácticas del pasado no son siempre la solución de amenazas futuras. Es posible que los que llevaron a cabo el ataque del 11 de septiembre usaran nuestros bien establecidos procedimientos para planear los secuestros contra nosotros mismos. Anteriores secuestradores habían usado las aeronaves y a los pasajeros como armas para negociar, no como bombas. La suposición de que los secuestros del 11 de septiembre seguirían ese modelo puede haber tenido como resultado que los pasajeros no resistieran a los secuestradores hasta que era demasiado tarde. Supón que tu enemigo está pensando como tú, y está realizando una posevaluación de las acciones y está buscando las formas de convertir tus medidas de seguridad en vulnerabilidades.

La evaluación de la vulnerabilidad debe examinar posibles puntos débiles que puedan surgir de la evaluación de una instalación. Los esfuerzos antiterroristas

para usar nuestras medidas de seguridad contra nosotros hacen necesario examinar minuciosamente los posibles efectos secundarios y terciarios de estas medidas y determinar en qué grado pueden ser predecibles. Estudia cada medida desde el punto de vista del terrorista para determinar de qué manera puede este, hacer que se vuelva contra nosotros mismos una medida implementada por nosotros. Por ejemplo, dejar esperando en fila a miles de militares fuera de la instalación mientras se procede al registro de todos los vehículos los hace fácilmente identificables como blancos estacionarios. Las medidas que hacen difícil entrar a un puesto militar también hacen difícil su evacuación en caso de un ataque químico o biológico. Lo predecible de nuestras respuestas es también una debilidad. Los terroristas son adversarios creativos que piensan.

Durante la última década hemos concentrado mucha energía en proteger a los EE.UU. de las armas de destrucción masiva y de ataques cibernéticos. El que hasta ahora no hayan ocurrido no quiere decir que no ocurran en el futuro, o que no debamos tomar las medidas necesarias para disuadirlos y para responder a dichos ataques. Es más, la atención que hemos puesto a estas amenazas de alta tecnología puede haber hecho desviar nuestra atención de otras formas de ataque menos sofisticadas, pero aún así, mortales. Este no es un problema de clasificación en escala, sino de un enfoque diferente. La disuasión o la respuesta en un caso determinado puede resultar inútil o contraproducente en otro. La evaluación de la vulnerabilidad debe examinar una amplia gama de amenazas. La necesidad de considerar no solamente el peor de los escenarios, sino también las amenazas que pueden variar de baja a alta tecnología y de simples a complejas.

Proteger nuestras instalaciones con el uso de la fuerza será una parte importante de nuestras vidas en un futuro inmediato. Si queremos tener éxito en nuestra empresa, tendremos que ser tan creativos como nuestro adversario. No podemos confiar simplemente en lo que ha dado resultados positivos en el pasado. Un enfoque sistemático en el desarrollo de los RIP, RIFF y EEIA llevado a cabo por personas creativas y dirigidos contra un enemigo creativo, contribuirá al cumplimiento de esta misión. **MR**

---

*El Coronel (Retirado) Clinton J. Ancker, III, Ejército de los EE.UU., es el Director de la Dirección de Doctrina de Armas Combinadas en la Escuela de Comando y Estado Mayor del Ejército de los EE.UU. (CGSC). Recibió el título de Bachiller de Ciencias de la Academia Militar de los EE.UU.; títulos de Maestría de las Universidades de Long Island, de Stanford y de la Escuela Superior de Guerra de la Armada de los EE.UU.; y es graduado de la CGSC. Ha servido en una variedad de posiciones de mando y estado mayor en Vietnam, Kuwait, Alemania y en el territorio continental de los EE.UU., entre las que se incluyen: Jefe de Equipo de Enlace Militar en Albania y Asistente del Comandante en Jefe del Comando de Operaciones Especiales en la Base Aérea de MacDill, en el estado de la Florida.*